Cassandra Crossing/ Invisibile Internet Project

(50)— Ecco cos'è e come funziona la rete invisibile insaccata dentro la rete, ora più facilmente utilizzabile. Ecco come iniziare ad…

Cassandra Crossing/ Invisibile Internet Project

Figure 1:

(50)— Ecco cos'è e come funziona la rete invisibile insaccata dentro la rete, ora più facilmente utilizzabile. Ecco come iniziare ad esplorare una singolare tipologia di darknet. I pro e i contro.

22 settembre 2006— I2P è l'acronimo di *Invisible Internet Project*, un'applicazione per la privacy il cui progetto è partito nell'ormai lontano 2003 e che nell'ultima release ha raggiunto una usabilità che permette di provarla a scopo sperimentale. Maggiori particolari sono reperibili su questa voce di Wikipedia ed in questo articolo.

La sigla è simile a quella di un altro progetto ormai defunto (IIP—Invisible IRC Project) ma si tratta di cosa completamente diversa e in via di rapido sviluppo.

I2P è un'applicazione scritta prevalentemente in Java che realizza una Darknet a livello applicativo, offrendo servizi interessanti ed un'interfaccia molto completa (vedi immagine più sotto).

I2P esiste sia in versione per GNU/Linux (e vari *nix) che per Windows, ed è scaricabile da qui. L'installazione nei due ambienti richiede ovviamente l'uso di una macchina virtuale Java (JVM); benché I2P dichiari di supportare anche Kaffe (l'unica JVM libera) non è stato possibile farla funzionare con Debian Etch; si consiglia quindi si usare la versione JRE 5 update 8 di Sun Microsystem, reperibile qui.

Per gli utenti Windows non ci sono particolari problemi, per quelli GNU/Linux si consiglia di eseguire una installazione locale della JVM e di utilizzare la variabile PATH per far ricercare i file nella directory della JVM prima che in quelle standard, dando, prima di lanciare I2P, un comando tipo:export PATH=~/jre1.5.0_06/lib:~/jre1.5.0_06/bin:$PATH

Figure 2:

Una volta lanciata l'applicazione, è possibile collegarsi con un browser al link dell'interfaccia di amministrazione di I2P (raggiungibile solo con I2P installato) dove, rinfrescando la pagina, si dovrebbe vedere il numero dei peers salire in pochi minuti, ovviamente solo se siete su una connessione ragionevolmente aperta; in caso contrario consultate l'apposito link presente nella pagina sulla configurazione dei firewall.

Per visitare i link interni ad I2P, iniziando da quelli elencati nella pagina, dovete configurare il browser sul proxy 127.0.0.1:4444, escludendo l'indirizzo 127.0.0.1 da quelli che usano il proxy a pena il non poter utilizzare più l'interfaccia di controllo.

E' ora possibile visitare i "siti web" interni alla Darknet di I2P, che sono contraddistinti da un top level domain.i2p e chiamati "eepsite"; questi eepsite spesso non sono disponibili, sia perché la rete I2P è ben lontano dalla stabilità e disponibilità di altre reti quali Tor o Freenet, sia perché gli eepsite non sono in realtà distribuiti ma si trovano su singole macchine in quel momento collegate alla Darknet di I2P.

E' possibile creare e pubblicare un proprio eepsite senza nessuna ulteriore configurazione, seguendo le semplici istruzioni del link MyEepsite sulla home dell'interfaccia di amministrazione.

Per meglio definire le caratteristiche di I2P è opportuno confrontarla con altri due software per la privacy molto più noti, Tor e Freenet 0.5. Sul sito di I2P è presente un documento che esegue una comparazione, non completamente esaustiva ed a tratti discutibile ma comunque meritevole di lettura, con Tor, Freeenet ed altre applicazioni per la privacy.

I2P realizza una Darknet a livello applicativo, non di rete come Tor od in maniera più complessa Freenet 0.5; questo significa che per utilizzare l'anonimato garantito da I2P ci si può muovere esclusivamente all'interno dell'applicazione stessa. Non è possibile utilizzare applicazioni internet standard (come ad esempio IRC o mail) direttamente attraverso la Darknet di I2P, come è possibile con Tor.

Esistono tuttavia degli eepsite proxy per particolari servizi, quali ad esempio IRC, SMTP, POP3, Torrent, che consentono di usarli sia internamente ad I2P che con internet; sono comunque funzionalità molto diverse e più limitate di quelle realizzate da Tor, perché questi servizi, sia nella rete I2P che su Internet, passano dal server che ospita il relativo proxy, che è quindi suscettibile ad attacchi DoS, e deve essere necessariamente disponibile e fidato.

Uno dei proxy pubblicati sulla homepage consente di utilizzare un nodo Freenet 0.5, agendo da vero e proprio gateway tra le due Darknet; un approccio molto interessante, non solo da un punto di vista pratico ma anche "filosofico".

Al contrario di Freenet 0.5 ed analogamente a Tor, I2P non possiede un datastore, cioè la capacità di memorizzare dati in maniera ridondante e distribuita, ma si affida ad uno schema comune in programmi P2P tipo Gnutella, di far risiedere ogni file su una particolare macchina collegata ad I2P, ed anonimizzarne solo la ricerca e l'accesso.

Il livello di sviluppo di I2P potrebbe essere definito pre-Alpha, ed il suo utilizzo è vincolato ad una rete di pochi server spesso anche di bassa disponibilità; sembrerebbe che l'interesse legato alla nuova release di I2P, la prima per cui c'è stato un annuncio sulla stampa, abbia saturato l'intera rete I2P la cui disponibilità è drasticamente scesa durante questa settimana.

Come al solito troppi curiosi e poche persone disposte a condividere le proprie risorse, ma questo è un vecchio discorso. Si tratta comunque ancora di un'applicazione che, benché interessante, deve essere assolutamente evitata da chiunque desideri privacy ed anonimato ben garantiti.

Rimangono da segnalare due problemi legati allo sviluppo di I2P:

1) Il licensing della parte principale di I2P è public domain, e non GPL od altra licenza libera; questo permette a chiunque di appropriarsi del codice sorgente e farne utilizzi commerciali. La ragione di questa scelta è probabilmente dovuta al fatto che I2P usa molte parti di altri software pubblicati con le licenze Open Source più svariate e difficilmente (per usare un eufemismo) conciliabili tra loro.

2) Il protocollo di I2P, come del resto quello di Freenet, non è concepito, documentato e verificato a priori; esso è quindi deducibile solo dal codice e da una scarsa e poco aggiornata documentazione. Questo rende il software concettualmente poco affidabile e difficilmente analizzabile, in particolare per quanto riguarda la sua robustezza e la resistenza agli attacchi ed alle compromissioni.

Per concludere: I2P è un oggetto interessante che merita senz'altro il tempo necessario per una prova. Merita anche di essere tenuto d'occhio nei suoi sviluppi futuri, ma per ora è ben lontano da poter fornire quel minimo di affidabilità che altre applicazioni per la privacy, come Tor, Freenet, Mixminion o Mixmaster hanno raggiunto.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.